SPYWOLF

Security Audit Report

Completed on

November 20, 2023

OVERVIEW

This audit has been prepared for **VAULTED** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

VAULTED

PROJECT DESCRIPTION

According to their website:

Vaulted is the easy and secure way to lock liquidity for your project on the Ethereum network - we make locking liquidity more efficient via our Dapp, which enables project developers to complete a fundamental task quickly and effectively.

As we all know, locking liquidity is a basic requirement for projects in the space, and our Dapp facilitates this in the most streamlined way possible.

Release Date: Presale starts in November, 2023

Category: Token

CONTRACT INFO

Token Name
Vaulted Finance

Symbol
VAULTED

Contract Address
0x254756364550A6cac7FE39CE73241bbbcF9a17E0

Network
Ethereum

Language
Solidity

Deployment Date
Nov 19, 2023

Contract Type
Token with taxes

Total Supply
1,000,000,000

Status
Not launched

TAXES

Buy Tax
3%

Sell Tax
3%

*Taxes will be higher in the first 14 blocks after initial token launch

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	7
Uniq Senders	3
Uniq Receivers	4
Total Amount	3484500054.6831326 VAULTED
Median Transfer Amount	742250011.6483154 VAULTED
Average Transfer Amount	497785722.0975904 VAULTED
First transfer date	2023-11-19
Last transfer date	2023-11-19
Days token transferred	1

SMART CONTRACT STATS

Calls Count	28
External calls	9
Internal calls	19
Transactions count	15
Uniq Callers	5
Days contract called	1
Last transaction time	2023-11-19 23:31:35 UTC
Created	2023-11-19 01:34:23 UTC
Create TX	0x7b3ad7f10aa328a020ee65409808343a0844fd8b2201a1d105834ed712b1ec0a
Creator	0x757c4bd256c051e51deae08d6e8351e3cf13daf1

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can activate trading once.
tradingActive is currently false, allowing vetted addresses to potentially sell their presale tokens before opening trade for the investors.

Note: This only applies if launching on a launchpad platform like Pinksale.

```
function openTrading() public onlyOwner {
    require(tradingOpenedOnBlock == 0, "token state is already live");
    tradingOpenedOnBlock = block.number;
    tradingActive = true;
    swapEnabled = true;
}
```

- Recommendation:
  - Once presale is finished and trading is not enabled, investors cannot sell their token holdings on token launch. Trading should be enabled before presale finish and token launch on DEX.

Informational

There are dynamic fees applied shortly after the initial token launch.
On the first 6 blocks after initial trade enabling, taxes will be 15% for buys and 30% for sells.
From 7th block after initial enable trading to 14th block, taxes will be 3% for buys and 20% for sells.
From block 15 after initial trading enable, taxes will be 3% for buy and 3% for sell. Taxes cannot be changed further on.

```
function openTrading() public onlyOwner {
    require(tradingOpenedOnBlock == 0, "token state is already live");
    tradingOpenedOnBlock = block.number;
    tradingActive = true;
    swapEnabled = true;
}

function getFees() internal {

    require(
        tradingOpenedOnBlock > 0,
        "Trading not live"
    );

    uint256 currentBlock = block.number;
    uint256 lastTierOneBlock = tradingOpenedOnBlock + 6;
    uint256 lastTierTwoBlock = tradingOpenedOnBlock + 14;

    if(currentBlock <= lastTierOneBlock) {
        buyTaxRate = 15;
        sellTaxRate = 30;
    } else if(currentBlock > lastTierOneBlock && currentBlock <= lastTierTwoBlock) {
        buyTaxRate = 3;
        sellTaxRate = 20;
    } else {
        buyTaxRate = 3;
        sellTaxRate = 3;
        fetchFees = false;
    }
}
```

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(
    address account,
    bool excluded
) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
}

function setAdminAddress(address account, bool status) external onlyOwner {
    _isAdminAddress[account] = status;
    _isExcludedFromFees[account] = status;
    _isExcludedMaxTransactionAmount[account] = status;
}

function setMultipleAdminAddresses(
    address[] calldata addresses,
    bool status
) external onlyOwner {
    for (uint256 i; i < addresses.length; ) {
        _isAdminAddress[addresses[i]] = status;
        _isExcludedFromFees[addresses[i]] = status;
        _isExcludedMaxTransactionAmount[addresses[i]] = status;
        unchecked {
            i++;
        }
    }
}
```

Informational

Owner can withdraw any tokens from the contract except ETH. When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function rescueTokens(address _token, uint256 amount) external {
    require(
        msg.sender == owner() || msg.sender == devWallet,
        "this address is not authorized to call this function"
    );
    IERC20(_token).transfer(devWallet, amount);
}
```

Owner can set max sell transaction amount but cannot lower it than 0.1% of total supply.

```
function updateMaxSellAmount(uint256 newNum) external onlyOwner {
    require(
        newNum >= ((totalSupply() * 1) / 1_000),
        "cannot set max sell amount lower than 0.1%"
    );
    maxSellAmount = newNum;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.......................
else if (
    to == UNISWAP_V2_PAIR && !_isExcludedMaxTransactionAmount[from]
) {
    require(
        amount <= maxSellAmount,
        "Sell transfer amount exceeds the max sell."
    );
}
.......................
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

VAULTED

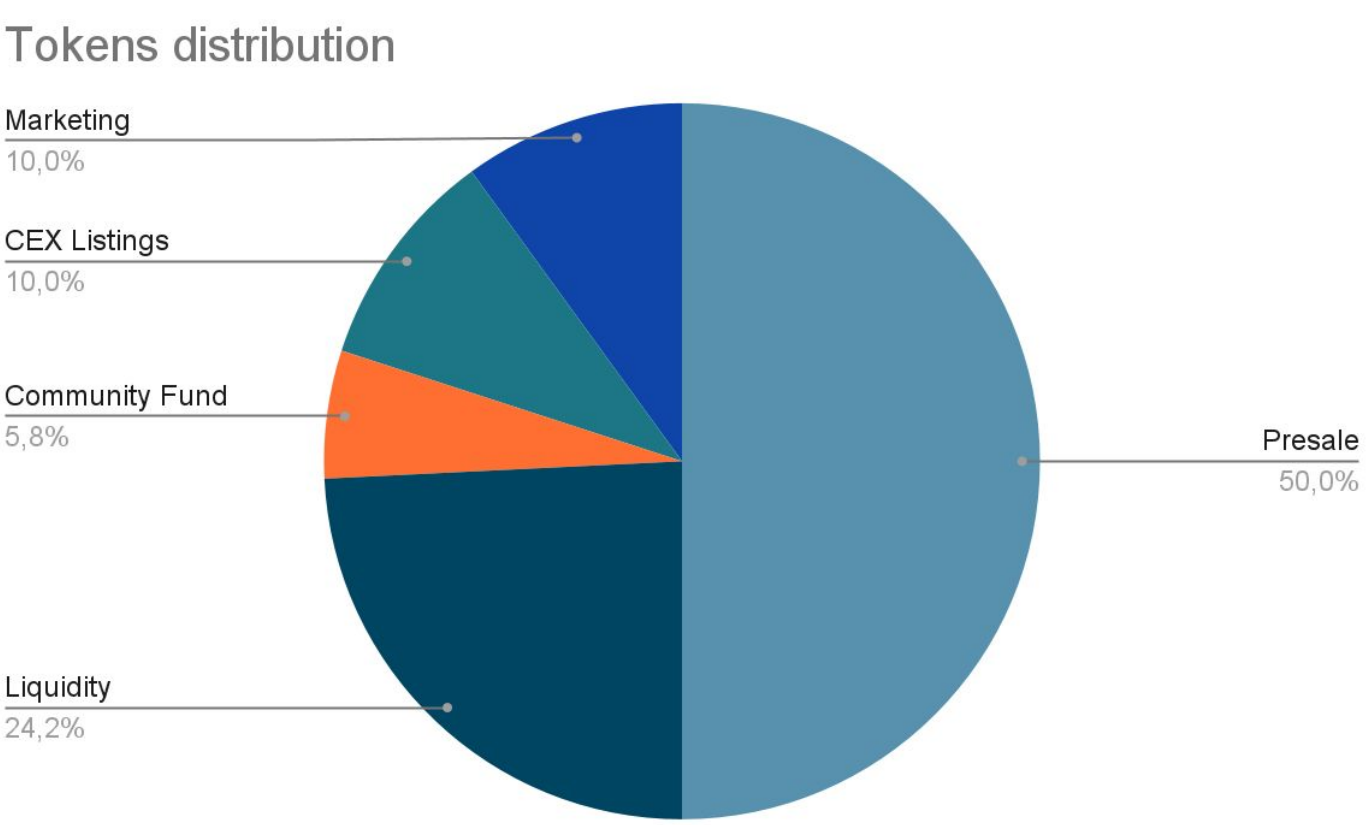
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but cannot lower it than 0.1% of total supply

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 50% - Presale
- 24.225% - Liquidity
- 5.775% - Community Fund
- 10% - CEX Listings
- 10% - Marketing



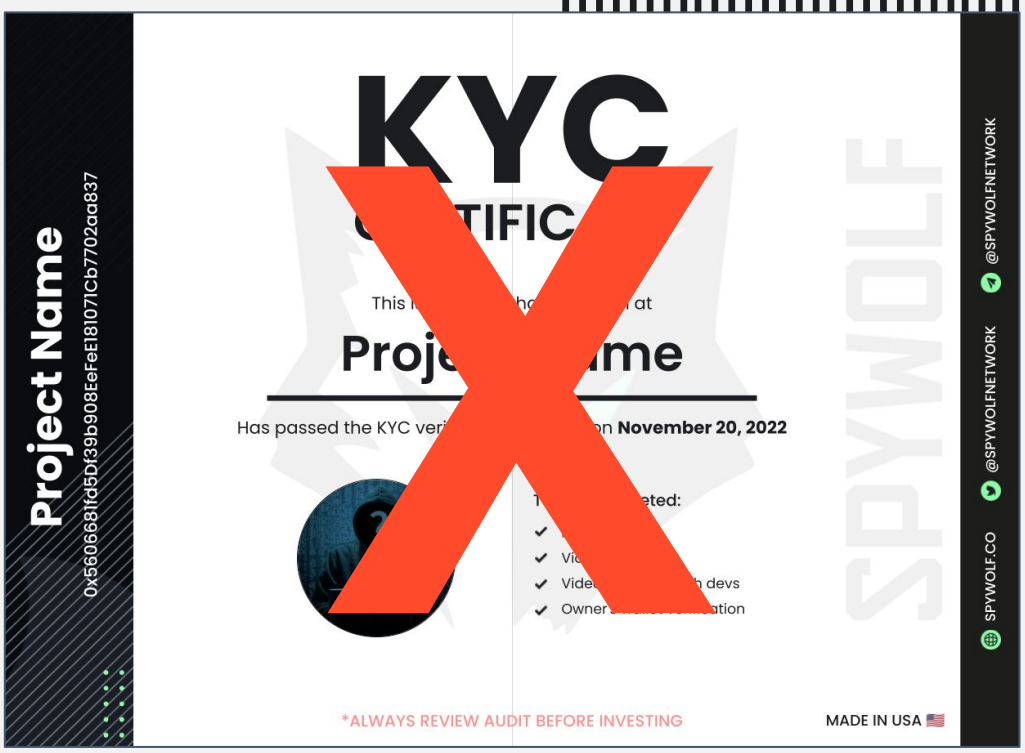
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://vaulted.finance/

Domain Registry
https://www.hostinger.com

Domain Expiration
2024-11-04

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

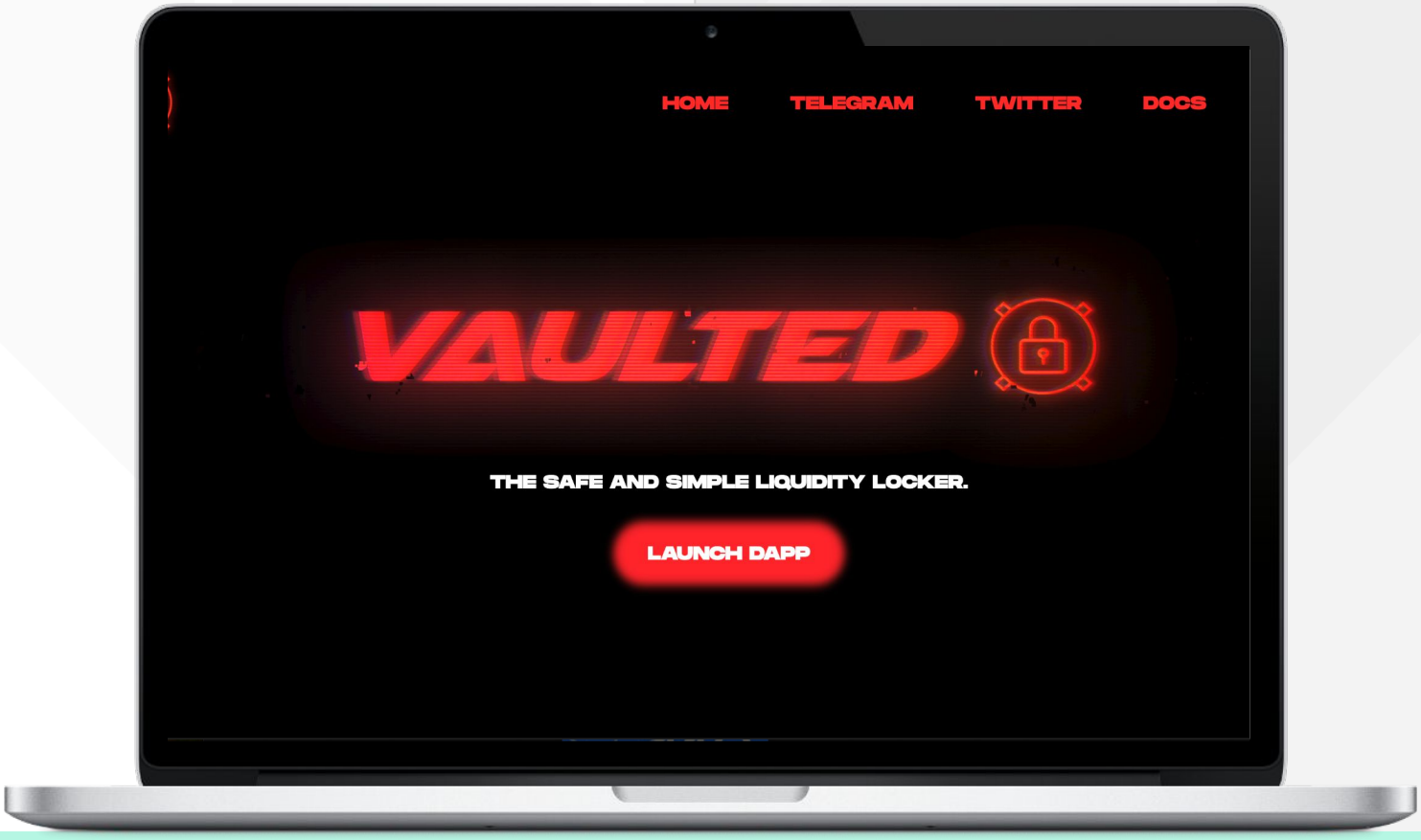
Design
Very nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written and explanatory documents page.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



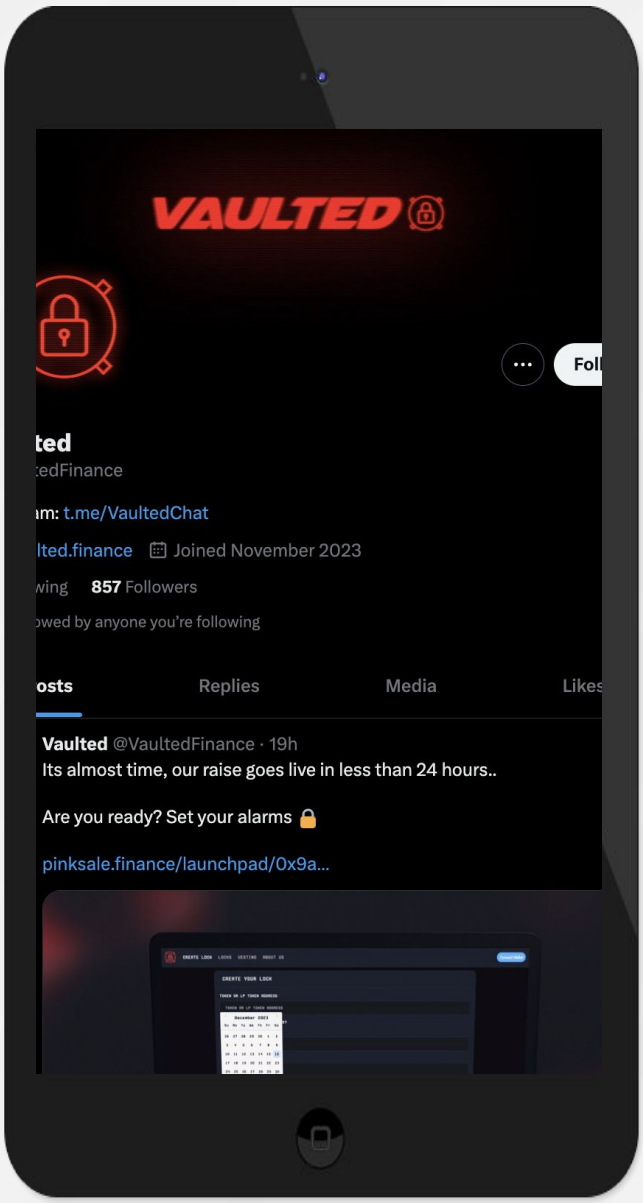
vaulted.finance

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are new



Twitter

@vaultedfinance

- 857 followers
- 4 total posts
- Active

Discord

- Not available

Telegram

@vaultedchat

- 393 members
- Active

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.